IN THE CLAIMS

What is claimed is:

1. (Currently Amended) A method for redirecting network message traffic comprising:

receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

rerouting all message traffic carried via the first transport mechanism in the communications network, and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex;

establishing a second transport mechanism having a separate set of routing tables in an overlay arrangement with the first transport mechanism under which the rerouting to the filter complex occurs; and

directing the filter~~ing~~ complex to transmit, via the~~a~~ second transport mechanism over the communications network, the desirable message traffic to the target node, directing the filter complex further comprising propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism, the second transport mechanism defining a Virtual Private Network (VPN) protocol.

2. (Previously Presented) The method of claim 1 further comprising directing the filter complex to filter the message traffic to subdivide desirable message traffic from undesirable message traffic.

3. (Original) The method of claim 1 wherein the filter complex further comprises a security filter having filtering logic for performing filtering, the security filter operable to parse the message traffic and identify sequences in the message traffic indicative of undesirable message traffic.

4. (Original) The method of claim 3 wherein the filter complex further includes a filter routing device in communication with other routing devices in the communications network and coupled to the security filter for analyzing message traffic.

5. (Currently Amended) The method of claim 4 wherein the filter routing device in the filter~~ing~~ complex is operable to communicate according to the first transport mechanism and the second transport mechanism.

6. Canceled

7. (Original) The method of claim 1 wherein directing further comprises directing a target node router serving the target node from the network management server, the network management server operable to send a redirect message to the target node router.

8. (Currently Amended) The method of claim 6 wherein the reroute message is indicative of the filter~~ing~~ complex receiving message traffic according to the first transport mechanism intended for the target node via the target node router serving the target node.

9. (Original) The method of claim 7 wherein the redirect message is indicative that the target router serving the target node is not to receive message traffic according to the first transport mechanism corresponding to the target node.

10. (Original) The method of claim 7 wherein the redirect message is indicative that the target node router serving the target node receives the desirable message traffic in the second transport mechanism corresponding to the target node.

11. (Original) The method of claim 1 wherein first and second transport mechanisms coexist on a common physical network.

12. (Original) The method of claim 1 wherein first transport mechanism corresponds to a public access protocol adapted for communication via a plurality of dissimilar network switching devices.

13. (Original) The method of claim 1 wherein the second transport mechanism corresponds to a virtual private network operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network.

Claims 14-15. Canceled

16. (Original) The method of claim 1 wherein rerouting all message traffic is a static route, according to the first transport mechanism, from a single router serving the target node to the filter router serving the filter complex.

17. (Previously Presented) The method of claim 1 wherein receiving an indication further comprises detecting a recognizable pattern of inundating undesirable message traffic.

18. (Original) The method of claim 1 wherein the undesirable message traffic emanates from a plurality of sources, each of the plurality of sources independently contributing substantially insignificant volume of message traffic.

19. (Currently Amended) A network management server for redirecting undesirable message traffic comprising:

a network intrusion detector monitor operable to receive an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

a routing processor operable to propagate routing information from a routing table database to reroute all message traffic using the first transport mechanism directed to the particular target node; and

a connection to a filter complex responsive to the routing processor, the filter complex operable to distinguish desirable message traffic from undesirable message traffic, and further operable to transmit, by redirecting the desirable message traffic via a second transport mechanism over the communications network, the desirable message traffic to the target node, the redirecting thus transporting the same message via both the first transport mechanism and the second transport mechanism;

the filter complex operable to reroute all message traffic including propagating, via a standard protocol corresponding to the first transport mechanism, a node address other than the node address corresponding to the target node,

the routing processor operable to direct the filter complex to propagate routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism, the second transport mechanism having a separate set of routing tables in an overlay arrangement with the first transport mechanism under which the rerouting to the filter complex occurs,

the second transport mechanism defining a Virtual Private Network (VPN) protocol,

the network management server further operable to send a reroute message to the filter complex, in response to which the filter complex is operable to reroute the message traffic, the reroute message indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node.

20. (Previously Presented) The network management server of claim 19 wherein the filter complex is further operable to filter the message traffic to subdivide the desirable message traffic from the undesirable message traffic.

21. (Original) The network management server of claim 19 wherein the filter complex further comprises a security filter having filtering logic for performing filtering, the security filter operable to parse the message traffic and identify sequences in the message traffic indicative of undesirable message traffic.

22. (Original) The network management server of claim 21 wherein the filter complex further includes a filter routing device in communication with other routing devices in the communications network and coupled to the security filter to analyze message traffic.

23. (Currently Amended) The network management server of claim 22 wherein the filter routing device in the filter~~ing~~ complex is operable to communicate according to the first transport mechanism and the second transport mechanism.

24. Canceled

25. (Original) The network management server of claim 19 wherein the routing processor is further operable to direct a target node router serving the target node from the network management server, the network management server operable to send a redirect message to the target node router.

26. Canceled

27. (Original) The network management server claim 25 wherein the routing processor is further operable to send a redirect message indicative that the target router serving the target node is not to receive message traffic according to the first transport mechanism corresponding to the target node.

28. (Original) The network management server claim 25 wherein the redirect message from the routing processor is further indicative that the target node router

serving the target node receives the desirable message traffic in the second transport mechanism corresponding to the target node.

29. (Original) The network management server of claim 19 wherein a network interface in the network management server is compatible with the first and second transport mechanisms and wherein first and second transport mechanisms coexist on a common physical network.

30. (Original) The network management server of claim 19 wherein first transport mechanism is operable according to a public access protocol adapted for communication via a plurality of dissimilar network switching devices.

31. (Original) The network management server of claim 19 wherein the second transport mechanism is operable according to a virtual private network protocol operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network.

32. (Original) The network management server of claim 19 wherein the filter complex is operable to reroute all message traffic including propagating, via a standard protocol corresponding to the first transport mechanism, a node address other than the node address corresponding to the target node.

33. (Original) The network management server of claim 19 wherein the routing processor is operable to direct the filter complex to propagate routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism.

34. (Previously Presented) The network management server of claim 19 wherein the routing processor is operable to rerouting the message traffic according to a static route in the first transport mechanism, from a single router serving the target node to the filter router serving the filter complex.

35. (Original) The network management server of claim 19 wherein the undesirable message traffic emanates from a plurality of sources, each of the plurality of sources independently contributing substantially insignificant volume of message traffic.

36. (Currently Amended) In a network management server of a networked system of data communications devices, a method for transparently intercepting, filtering, and rerouting message traffic for recovering from a distributed denial of service attack comprising:

detecting, at a network monitor in the network management server, a pattern of inundating undesirable message traffic to a particular target node transported via a first transport mechanism in a communications network;

receiving, via a routing processor, an indication of the undesirable message traffic directed to the particular target node;

transmitting, via a network interface, a reroute message to a filter complex having a security filter operable to distinguish desirable message traffic from undesirable message traffic; and

rerouting, via a filter routing device in the filter complex, all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filter~~ing~~ complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node;

establishing a second transport mechanism having a separate set of routing tables in an overlay arrangement with the first transport mechanism under which the rerouting to the filter complex occurs;

filtering, at the security filter, the message traffic to bifurcate desirable message traffic from undesirable message traffic;

transmitting, via the network interface to a target node router serving the target node, a redirect message indicating that the target node router is to receive, via the second transport mechanism, the desirable message traffic directed to the particular target node and rerouted to the filter complex, the filter complex and the target node router conversant in the first transport mechanism and the second transport mechanism, the second transport mechanism defining a Virtual Private Network (VPN) protocol; and

directing, from the network management server, the filter~~ing~~ complex to transmit, via the~~a~~ second transport mechanism over the communications network, the desirable message traffic to the target node, directing the filter complex further comprising propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism.

37. (Currently Amended) A computer program product having an encoded set of processor based instructions on a computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for directing a processor to perform steps for redirecting network message traffic comprising:

computer program code for receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

computer program code for rerouting all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from

undesirable message traffic, rerouting all message traffic further comprising propagating, via a standard protocol corresponding to the first transport mechanism, a node address other than the node address corresponding to the target node, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node;

computer program code for establishing a second transport mechanism having a separate set of routing tables in an overlay arrangement with the first transport mechanism under which the rerouting to the filter complex occurs; and

computer program code for directing the filtering complex to transmit, by redirecting the desirable message traffic via thea second transport mechanism over the communications network, the desirable message traffic to the target node, the redirecting thus transporting the same message via both the first transport mechanism and the second transport mechanism~~the first transport mechanism and the second transport mechanism having different sets of routing tables~~, directing the filter complex further comprising propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism, the second transport mechanism defining a Virtual Private Network (VPN) protocol.

38. (Canceled)

39. (Currently Amended) A network management server for redirecting undesirable message traffic comprising:

means for receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

means for rerouting all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node;

means for establishing a second transport mechanism having a separate set of routing tables in an overlay arrangement with the first transport mechanism under which the rerouting to the filter complex occurs; and

means for directing the filtering complex to transmit, by redirecting the desirable message traffic via thea second transport mechanism over the communications network, the desirable message traffic to the target node, the redirecting thus transporting the same message via both the first transport mechanism and the second transport mechanism, the second transport mechanism corresponding to a virtual private network operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network, the second transport mechanism defining a Virtual Private Network (VPN) protocol.

40. (New) A method of redirecting an inundation of undesirable message traffic in a computer network comprising:

establishing, in the computer network, a first protocol for routing general message traffic in the computer network;

establishing, in the computer network, a second protocol specific to a virtual private network (VPN), the second protocol having a separate set of routing tables in an overlay arrangement with the first protocol,

the second protocol having transport ability between at least a filter complex, a target node, and a target node router, the target node router included in a routing path to the target node, the target node router in communication with the target node via both the first protocol and the second protocol and operable to deliver message traffic to the target node via either the first protocol and the second protocol;

identifying an indication of undesirable message traffic directed to the target node via the first protocol in the computer network;

propagating routing information according to the first protocol, the routing information operable for redirecting the message by designating the filter complex in the routing path to the target node via routing in the first protocol; and

sending a reroute message to the filter complex, the reroute message operable to designate the target node as the destination of the message according to the second protocol,

redirecting including sending instructions to the target node router coupled to the target node, the instructions designating the target node router as a destination router for the target node according to the second protocol,

the redirecting thus transporting the same message via both the first protocol and the second protocol.

41. (New) The method of claim 40 wherein the first protocol and the second protocols are different protocols recognized in a Multi-Protocol Layer Service (MPLS) network.

42. (New) The method of claim 19 wherein the first and second transport mediums are protocols, the first protocol and the second protocols being different protocols recognized in a Multi-Protocol Layer Service (MPLS) network.